BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-1101
1 MAY 1997

Operations

★*OPERATIONS SECURITY*

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

This instruction implements Air Force Policy Directive (AFPD) 10-11, *Operations Security*; DoD Directive 5205.2, *DoD Operations Security Program,* July 7, 1983; Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3210.01, *Joint Information Warfare Policy*, January 2, 1996; CJCSI 3213.01, *Joint Operations Security,* May 28, 1993; and Operations Security requirements for DoD Instruction 5000.2, *Defense Acquisition Management Policies and Procedures,* February 23, 1991 with Change 1. It provides guidance for all Air Force personnel and supporting contractors in implementing and maintaining OPSEC programs. It describes the OPSEC process, and discusses integration of OPSEC into Air Force plans, operations, and support activities.

SUMMARY OF REVISIONS

★This revision introduces the supporting role of theOperations Security (OPSEC) process in the military's emerging information warfare arena; eliminates MAJCOM and Air Force Information Warfare Center (AFIWC) status reporting requirements; streamlines definitions and program descriptions to reduce document redundancy; and provides flexibility to AFIWC training curriculum development by eliminating syllabus mandates.

Paragraph

Supersedes: AFI 10-1101, 19 May 1994.
OPR: HQ USAF/XOOP (Maj Milton Ganison III)

Certified by: HQ USAF/XOO (Maj Gen T. J. Schwalier)
Pages: 15/Distribution: F

Chapter 1

INTRODUCTION

1.1. Definition. OPSEC is a process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by potential adversaries.
- Determine indicators that could be interpreted or pieced together to derive critical information in time to be useful to an adversary.
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

1.2. Characteristics of OPSEC. The goal of OPSEC is to control information and observable actions about mission capabilities, limitations, and intentions in order to prevent or control exploitation by an adversary. Operational effectiveness is enhanced when OPSEC is applied by commanders and other decision makers during the earliest stages of planning. OPSEC provides a step-by-step analysis of operations and behavior, from an adversarial point of view, to determine how vulnerabilities might be exploited in time to be of use to an adversary. Information that adversaries need to achieve their goals to our detriment constitute the critical information of our operation or program. By identifying and denying this critical information, the OPSEC process becomes a positive, pro-active means by which adversaries are denied an advantage.

1.2.1. The OPSEC analysis examines the planning, preparation, execution, and post execution phases of any activity across the entire spectrum of military activity, and in any operating environment. Air Force commanders and decision makers should consider OPSEC during both mission and acquisition planning.

1.2.2. OPSEC should be closely coordinated with security disciplines (Physical Security, AFI 31-4; *Information Security*, AFI 31-4, and *Information Protection*, AFI 33-2) to ensure that all aspects of sensitive activities are protected. Potential exploitation of open sources and observable actions are a primary focus of OPSEC analysis. These sources are generally unclassified and, consequently, more difficult to control. The analysis facilitates risk management by providing decision makers with a means of directly assessing how much risk they are willing to accept.

1.3. Air Force Operations Security. The Air Force implements the OPSEC process in all functional areas. Commanders are responsible for OPSEC awareness throughout their organizations and for integrating the OPSEC process throughout appropriate mission areas.

1.3.1. OPSEC is an integrated component of information warfare (IW). It provides a means of detecting and controlling an adversary’s actions on our military information functions. OPSEC assists in protecting IW capabilities and intentions from adversary knowledge and attack.

1.3.2. In acquisition, research and development efforts are enhanced through reduction in compromised technology and proprietary information. Organizations that fail to implement OPSEC are more likely to unintentionally give away critical information and expose missions to increased risk.

1.3.3. OPSEC should be considered simultaneously with complementing and competing activities to obtain maximum effectiveness. Planners and decision makers should consider operational objectives, strategies, deception, psychological operations, electronic warfare, and traditional security measures as a single effort to control the perception, decisions and activities of an adversary.

Chapter 2

THE OPERATIONS SECURITY PROCESS

2.1. General. The OPSEC analysis is accomplished through the use of a five-step process. The five steps of the OPSEC process are:

- Identification of Critical Information (and its indicators).
- Analysis of Threats.
- Analysis of Vulnerabilities.
- Assessment of Risk.
- Application of Appropriate Measures.

These steps are normally applied in a sequential manner during deliberate planning, however, dynamic situations may require any one to be revisited at any time

2.2. Identification of Critical Information. Critical information is information about friendly (U.S., allied, and/or coalition) activities, intentions, capabilities or limitations that an adversary needs in order to gain a military, political, diplomatic, or technological advantage. Such information, if released to an adversary prematurely, may prevent or forestall mission accomplishment, reduce mission effectiveness, or cause loss of lives and/or damage to friendly resources. Critical information usually involves a few key items of friendly activities or intentions that might significantly degrade mission effectiveness. Critical information may also be derived from bits and pieces of related information (indicators).

2.2.1. Critical information is best identified by individuals responsible for the development and execution of the operation. They possess the intimate familiarity necessary to properly apply the OPSEC process to the task at hand.

2.2.2. Mission critical information is to be identified at the earliest possible time, preferably during the conceptual planning phase of an activity. Subordinate and supporting organizations should be notified to control the identified critical information and unique *indicators* of that critical information.

2.2.3. A list of critical information will be developed and appropriately revised to reflect changing situations. Critical information is usually only critical for a prescribed period of time. The need to control or protect specific items of information will most likely change as the operation progresses and/or as the threat changes.

2.2.4. The Air Force will identify contractor requirements to control and protect certain critical information. Contractors will continue to control such information until the need for OPSEC measures no longer exist.

2.3. Threat Analysis. Current threat information is extremely important in developing appropriate OPSEC measures. This information is available from authorized USAF and DoD intelligence and counterintelligence organizations. An OPSEC threat analysis includes identifying adversaries and their capabilities, limitations, and intentions to collect, analyze, and use critical information and OPSEC indicators against friendly forces. This analysis must be tailored to the operation, test, activity, geographic region, or facility.

2.3.1. The Air Force Office of Special Investigations (AFOSI) produces counterintelligence studies and analyzes multi-disciplined intelligence threats posed to US Air Force and DoD programs and resources by foreign intelligence services. Local AFOSI detachments should be contacted to request counterintelligence studies or Multi-discipline Counterintelligence Threat Assessments (MDCI).

2.4. Vulnerability. An operations security vulnerability exists when friendly actions provide indicators that may be obtained and evaluated by an adversary in time to provide a basis for effective decision making. Once identified, conditions can normally be controlled.

2.5. Risk Assessment. Risk assessment involves an informed estimate of an adversary’s capability to exploit a friendly weakness; the potential effects such exploitation will have on operations, activity, or weapon system, and a cost-benefit analysis of actions contemplated to counter the vulnerability. Risks are reduced or eliminated by employing OPSEC measures to control the availability of information to the adversary.

2.5.1. OPSEC program managers, in concert with other planners, and with the assistance of intelligence and counterintelligence organizations, will provide risk assessments and recommendations to commanders (the senior decision makers). Commanders must decide whether or not to employ OPSEC measures.

2.5.1.1. The centerpiece of OPSEC is risk management. Recommended actions (OPSEC measures) are designed to preserve effectiveness of military capabilities while controlling the adversarial exploitation of critical information to the maximum extent possible.

2.6. OPSEC Measures. OPSEC measures are employed to counter or eliminate vulnerabilities that point to or divulge critical information. They help deny critical information by controlling the raw data adversaries use to make decisions, limiting their effectiveness, and possibly credibility. OPSEC measures enhance friendly capabilities by increasing the potential for surprise and effectiveness of friendly military forces and weapon systems.

2.6.1. Sometimes it may not be cost-effective or possible to alter the source of an OPSEC indicator. In these circumstances, attempts to disrupt or confuse the adversary’s ability to collect and/or properly interpret the information may be required. OPSEC measures should also be considered as a means to influence the adversary and their ultimate comprehension or use of the information when an indicator cannot be modified.

2.6.2. OPSEC measures can be used to eliminate the source of indicators or vulnerability of friendly actions to exploitation by adversary intelligence systems through action control. Specifically, select what actions to undertake; decide whether or not to execute actions necessary to accomplish tasks. When it is impossible or impractical to use action control procedures, countermeasures may be employed to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use unit, system designs, and procedures to create diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering and processing capabilities. A third method is to employ counteranalysis. The objective of counteranalysis is to prevent accurate interpretation of indicators during adversary analysis of collected materials. This is done by confusing the adversary analyst through deception techniques such as covers. Finally, protective measures are methods to create closed information systems to prevent adversaries from gaining access to information and resources. Examples include cryptologic systems and standardized security procedures.

Chapter 3

AIR FORCE OPERATIONS SECURITY PROGRAM

3.1. Purpose. To provide Air Force decision makers at all levels with a means of promoting understanding and awareness in the integration and application of OPSEC. The Air Force OPSEC Program provides all commands with standardized policy to facilitate effective OPSEC programs. An OPSEC program manager is identified within Air Staff to advise on the integration of OPSEC into Air Force plans and directives; develop policy and guidance that provides for the coordination, training, education, and recognition of all unit OPSEC programs.

3.2. Training and Education. The purpose of OPSEC training and education is to ensure Air Force people understand:

- The positive benefits of OPSEC.
- The effects of foreign intelligence collection on mission effectiveness.
- What the Air Force does to control the exploitation of critical information. The OPSEC program provides Air Force members with a general knowledge of the OPSEC process and application.

3.2.1. OPSEC Education is a continuing requirement and must be provided to personnel upon their initial entrance into military service (via Basic Military Training School, Reserve Officer Training Corps, Officer Training School, the Air Force Academy, etc.) as well as to civilian employees, through Civilian Personnel channels, as they are brought into Federal Service.

3.2.2. Education topics must include the purpose of OPSEC, the OPSEC process, the OPSEC program; the intelligence process, collection methods, and current collection activities.

3.2.3. Foreign Intelligence. Sources for foreign intelligence support to OPSEC include AFIWC, local and MAJCOM intelligence organizations, and AFOSI.

3.2.4. Counterintelligence. AFOSI is the USAF agency responsible for counterintelligence and MDCI threat assessments. They produce studies, estimates, and analyses in support of the OPSEC program. Such data includes information relating to the capabilities, intentions, resources, doctrine, and collection methods of foreign intelligence services or international terrorist activities.

3.2.5. OPSEC Program Manager (PM) Training. Job specific training is required for all individuals designated as OPSEC PMs, personnel assigned to AFIWC in support of the Air Force OPSEC program, and those who conduct formal OPSEC surveys. OPSEC training should be received within ninety days of initial assignment. The office of primary responsibility (OPR) for OPSEC training is AFIWC/OSW.

3.3. Funding. HQ USAF/XO will program for and fund the HQ USAF OPSEC Program billets and associated activities deemed necessary to orchestrate the Air Force OPSEC program.

3.4. Policy and Evaluation. HQ USAF/XOOP coordinates and evaluates policy for the Air Force OPSEC Program based on Department of Defense and joint policy guidelines, feedback received from Inspectors General (IG) reports, trends identified by AFIWC/OSW through organizational surveys, and feedback recieved from OPSEC PMs.

3.5. Coordination. HQ USAF/XOOP coordinates OPSEC programs and activities across MAJCOM lines of authority and with organizations outside the Air Force. A direct working relationship also exists between HQ USAF/XOOP, AFIWC/OSW, HQ AFOSI/XOQ, MAJCOMs, FOAs, and DRUs.

Chapter 4

UNIT OPERATIONS SECURITY PROGRAMS

4.1. Purpose and Composition. Effective unit OPSEC programs fully support the commanders efforts to achieve a successful and effective mission. Each program is composed of an OPSEC PM (the facilitator), OPSEC plans, funding, training, and feedback. OPSEC programs must have the following requisite aspects or capabilities:

4.1.1. Command Involvement. Commanders are responsible for ensuring OPSEC guidance is developed early in the planning and coordination process. Commanders may delegate authority for OPSEC program management, but should personally make risk management decisions regarding the implementation of OPSEC measures.

4.1.2. Operational Orientation. The OPSEC program is an operations management program and its goal is mission effectiveness. The emphasis is on OPERATIONS with the target objective being the “overall integrity” of a successful mission. The office of primary responsibility (OPR) should reside in the Plans or Operations element of the organization to ensure effective implementation across organizational and functional lines.

4.1.3. Integration. OPSEC should be integrated into all organizational plans and activities. Staff elements and supporting organizations must ensure OPSEC procedures are appropriately incorporated--at the earliest possible time--into all operations plans (OPLANs), concept plans (CONPLANs), operations orders, exercise plans, Mission Needs Statements (MNS), Operational Requirements Documents (ORD), operating procedures, operations, exercises and other plans and activities to consistently control critical information and OPSEC indicators.

4.1.4. Coordination. Individuals must protect critical information at all sources and at all levels. Coordination across functional and organizational lines facilitates OPSEC planning and enhances the effectiveness of OPSEC measures. In addition, commanders and/or OPSEC PMs must closely coordinate with intelligence and counterintelligence organizations to identify potential adversaries, intelligence collection capabilities and intentions, and support OPSEC survey efforts.

4.1.5. Self Inspection. MAJCOM program managers will accomplish annual self-inspections of OPSEC programs and requirements. Other PMs are encouraged to do the same. Self-Inspections will be tailored to the functions of the organization.

4.2. Operations Security Program Managers. Program managers will be assigned IAW AFPD 10-11. All other units are *encouraged* to assign managers depending upon their operational relationships. If OPSEC is assigned as an additional responsibility, it should be combined with other activities providing synergistic mission enhancement.

4.2.1. In the acquisition environment, OPSEC program managers should work directly with program directors to ensure OPSEC principles are integrated and applied throughout the life-cycle of all programs.

4.2.2. OPSEC program managers are responsible for advising commanders (and/or program directors) on OPSEC related matters, facilitating OPSEC implementation, and managing the organization’s OPSEC program.

4.2.3. OPSEC PMs must be familiar with unit goals, objectives, strategies, activities, and personnel who participate in those activities.

4.3. OPSEC Planning. All Air Force organizations conducting or supporting operational missions must integrate OPSEC into plans or develop OPSEC plans to ensure mission critical information, information sources, and OPSEC indicators are protected.

4.3.1. OPSEC requires deliberate and continuous planning. Deliberate planning ensures OPSEC is implemented in a proactive manner and integrated into all operations and support activities. Continuous planning ensures flexibility and improvements during changing missions and threats.

4.3.2. OPSEC Plans. An OPSEC plan can be a separate plan, an annex to a larger plan, or the integration of OPSEC into an overall mission plan. OPSEC considerations include, but are not limited to:

4.3.2.1. Direction for participating organizations to protect critical information and the indicators of such information to prevent exploitation. Specific sources and associated OPSEC indicators may be different for each functional activity in an organization.

4.3.2.2. Critical information and OPSEC vulnerabilities applicable to the mission. OPSEC planners must consider adversarial objectives, the knowledge they need to effectively plan against friendly forces, and their capability to gain such information.

4.3.2.3. Direction to continuously monitor and review friendly activities to identify changing parameters as the operation matures.

4.3.2.4. Intelligence Threat Information. Air Force foreign intelligence and counterintelligence organizations will provide this information and should include the following:

- Adversarial intelligence collection capabilities, presence, and intentions. These factors must be continually assessed throughout the duration of each operation.
- Critical Information (CI). When CI pertinent to the existing or planned situation are known, they will be listed.
- Probable adversary knowledge. OPSEC planners should consider knowledge an adversary already has about a situation (from general knowledge, open source information, or from what they will know when the plan is implemented) to determine OPSEC vulnerabilities.

4.3.2.5. OPSEC Indicators. OPSEC plans should address indicators of critical information which are not currently protected.

4.3.2.6. OPSEC Measures. Once indicators are identified, OPSEC measures should be developed and applied to minimize or eliminate such indicators.

4.3.2.7. Coordination. OPLANs must be appropriately coordinated with supporting organizations to ensure critical information is consistently protected. Since exploitable information resides in numerous sources in most Air Force organizations and activities, OPSEC plans must be developed, coordinated, and implemented by all functional areas.

4.3.2.8. Subordinate and supporting organizations. When appropriate, subordinate and supporting organizations should develop supporting plans for their level and specific activities. MAJCOM, NAF, and wing plans will identify supporting organizations which are required to have a written OPSEC plan.

4.4. Unit OPSEC Training. The purpose of OPSEC training is to ensure personnel are familiar with potential threats related to the unit; critical information for the missions it supports, job specific OPSEC indicators; and the OPSEC measures they will execute.

4.4.1. Training will be developed and presented to newly assigned personnel within 90 days after arrival for duty. As a minimum, it should include:

- Duty related mission critical information and OPSEC indicators.
- Foreign intelligence threat to missions supported and conducted.
- Individual responsibilities.

4.5. Funding. All MAJCOMs, laboratories, product and logistics centers, and test ranges should program for and fund OPSEC billets. AFIWC will fund for and provide training aids and materials for use by OPSEC program managers throughout the Air Force infrastructure.

4.6. Evaluations. There are several methods used to evaluate OPSEC programs and the effectiveness of OPSEC measures:

- OPSEC Surveys
- Telecommunications Monitoring
- OPSEC Appraisals
- Inspector General Evaluations

4.6.1. OPSEC Surveys. Within this program, the terms survey and assessment are synonymous. Surveys are snapshots of an organization's OPSEC posture. There are two forms of surveys, OPSEC Multi-disciplinary Vulnerability Assessments (OMDVA), and in-house surveys.

4.6.1.1. The Air Force Information Warfare Center (AFIWC) is the only Air Force agency authorized to conduct OPSEC surveys across organizational boundaries. AFIWC/OSW conducts OMDVAs using a multi-disciplinary approach.

AFIWC/OSW personnel, along with augmentation from other organizations, contribute expertise and manpower for these in-depth surveys. HQ USAF, MAJCOMs, and local units (through MAJCOM channels) may request OPSEC surveys directly to AFIWC/OSW.

NOTE: The resources and time required to perform an in-depth OPSEC survey of this caliber severely limits the number of potential surveys during any one given year.

4.6.1.2. Commanders may conduct an in house survey with available resources. These surveys are normally conducted by the OPSEC program manager with support of functional area specialists from the organization or local area. The use of this type of survey is encouraged when scheduling or ops tempo do not provide the opportunity for an OMDVA.

4.6.2. Telecommunications Monitoring. Telecommunications monitoring involves the electronic monitoring and analysis of unsecure voice, fax and other electronic transmissions to estimate an organization's OPSEC posture. Telecommunications monitoring is accomplished only within certain legal parameters and may only be performed by authorized agencies as outlined in AFI 33-219 Telecommunications Monitoring and Assessment Program (TMAP). AFIWC surveys may include telecommunications monitoring.

4.6.3. OPSEC Appraisals. A timely OPSEC assessment is normally conducted in support of a specific operation, activity, or exercise. The appraisal is distinguished from the survey by the timeliness required for threat and vulnerability analysis and the application of OPSEC measures. It may be as limited as a desktop analysis in response to an operational planner's query, or as extensive as the formation of a multi-disciplined appraisal team to support a contingency, exercise, or field operational test and evaluation event. It may be conducted as a follow up to an OPSEC survey, or to provide a basis for initiating command or formal surveys.

4.6.4. Inspector General Evaluations. The extent to which Air Force components maintain their OPSEC programs will be a key area for evaluation during visits by inspectors general. Areas of interest will include: commanders' involvement, the integration of OPSEC into plans and operating procedures, training, program placement, intelligence support and counterintelligence support to the OPSEC program. Additional guidance is provided in the IG Instruction AFI 90-201, *Inspector General Activities*, concerning "common core criteria". MAJCOM/FOA/DRU PMs should coordinate with their respective IG team to ensure OPSEC evaluation criteria is current and IAW any unique guidance from the MAJCOM/FOA/DRU commander.

JOHN P. JUMPER, Lt General, USAF
DCS/Air & Space Operations

GLOSSARY OF TERMS

Terms

Capability —The ability to execute a specified course of action. (A capability may or may not be accompanied by an intention) (Joint Pub 1-02). **NOTE:** When considering vulnerabilities, a capability requires the physical and mental attributes and sufficient time required for performance.

Command and Control Warfare (C2W) —The integrated use of Operations Security (OPSEC), Military Deception, Psychological Operations (PSYOP), Electronic Warfare (EW), and Physical Destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and Control Warfare is an application of information warfare in military operations and is a subset of information warfare. Command and Control applies across the operational continuum and all levels of conflict.

Counteranalysis—Methods to effect the observation and/or interpretation of adversary intelligence analysts. Examples are military deceptions and covers. The objective is to prevent accurate interpretations of OPSEC indicators during adversary data analysis. This is done by confusing the adversary analyst through deception techniques.

Counterintelligence —Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Exploitation —a. Taking full advantage of success in battle and following up initial gains. b. Taking full advantage of any information that has come to hand for tactical or strategic purposes. c. An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. (Joint Pub 1-02)

Foreign Intelligence—Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence (except for information on international terrorist activities).

Information Function—Any activity involving the acquisition, transmission, storage, or transformation of information. (Cornerstones of Information Warfare)

Information Operations—Actions taken to effect adversary information and information systems while defending one's own information, and information systems. (DoD Directive 3600.1,*Information Operations*)

Information Warfare—Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (DoD Directive 3600.1)

Intelligence System—Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks. (Joint Pub 1-02)

Multi-discipline Counterintelligence Threat Assessment (MDCI)—All-source (HUMINT, SIGINT, and IMINT) analysis of threats to a specific activity, location, operation, project, weapons or other system, deployment, or exercise.

OPSEC Vulnerability—A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (Joint Pub 1-02)

RESPONSIBILITIES AND AUTHORITIES

A2.1. Command Responsibilities. Though the OPSEC program helps commanders to make and implement decisions, the decisions themselves are the commanders' responsibility. Commanders must understand the risk to the mission and then determine whether OPSEC measures are required. Commanders must make the difficult decisions that involve risks to mission effectiveness.

A2.1.1. Commanders at every level will:

- Integrate the OPSEC concept into their mission plans and activities.
- Ensure assigned personnel are familiar with OPSEC, and its application to organizational effectiveness.
- Ensure OPSEC measures are appropriately developed and executed to reinforce the combat effectiveness of units, defense systems and weapon systems.
- Centrally manage OPSEC guidance concerning critical information to ensure consistency throughout each organization and across organizational lines.

A2.2. Headquarters, United States Air Force (HQ USAF) Responsibilities. The Deputy Chief of Staff for Air & Space Operations (HQ USAF/XO) is the office of primary responsibility for the Air Force OPSEC program. HQ USAF/XO, through the Technical Plans Division (HQ USAF/XOOP), will:

- Develop OPSEC doctrine, policies, plans, and procedures consistent with joint and DoD OPSEC guidance.
- Designate an overall Air Force OPSEC Program Manager.
- Provide to J-3, Joint Staff, Attn: J-33/STOD/TSB, copies of all current Service OPSEC program directives and/or policy implementation documents.
- Support the National and DoD OPSEC programs as necessary.
- Provide management and annual review of the Air Force OPSEC Program.
- Recommend to the Deputy Under Secretary of Defense (Policy) for Policy Support changes to policies, procedures and practices of the DoD OPSEC Program.
- Utilize OPSEC training, advice, and service provided by the National Security Agency (NSA) and the Interagency OPSEC Support Staff (IOSS) when appropriate.

A2.2.1. HQ AFOSI will, upon request from the commander concerned, provide Air Force units with current mission specific counterintelligence and MDCI threat assessment information.

A2.3. Air Force Major Command (MAJCOM), Field Operating Agency (FOA), and Direct Reporting Unit (DRU). MAJCOMs, FOAs, and DRUs will develop effective OPSEC programs that meet the specific needs of their assigned missions and accomplish the following:

- Provide coordination across organizational boundaries as necessary (both vertically and horizontally) to ensure critical information and OPSEC indicators are consistently controlled and that OPSEC measures are effectively implemented and/or adhered
- Designate a program manager and an office of primary responsibility IAW AFPD 10-11. The decision to assign a full-time OPSEC program manager at FOAs and DRUs rests with the commander based upon the specific needs of the assigned mission.
- Ensure mission critical information is identified for each operation, activity, and exercise whether it be planned, conducted or supported.
- Develop OPSEC requirements for new weapon and/or defense systems in the acquisition cycle, list such requirements in Mission Needs Statements, and participate in milestone reviews to ensure such requirements are satisfied.
- Develop and cultivate the relationships necessary to ensure intelligence and counterintelligence support requirements for OPSEC programs.
- Provide guidance to subordinate units for controlling critical information and OPSEC indicators and ensure subordinate commands plan and exercise mission specific OPSEC measures.
- MAJCOM PMs will ensure OPSEC training of program managers (both full and part-time) at bases, laboratories, product and logistic centers, test ranges, and MRTFBs on a recurring basis.
- Ensure job oriented and mission specific OPSEC training is provided to all personnel on a recurring basis, as often as necessary, but not less than at one year intervals.
- MAJCOMs PMs will conduct annual OPSEC self-inspections to assess their OPSEC programs.

A2.4. Air Force Information Warfare Center. Air Force Information Warfare Center (AFIWC) will provide administrative support, technical services, and assistance for OPSEC program development, planning, and execution. The focal point for OPSEC support and expertise within AFIWC is the C2W Operations Division (OSW). Direct communication is authorized between AFIWC/OSW and the MAJCOM, FOA, and DRU OPSEC program managers. Informal communication is authorized between AFIWC/OSW and other Service and DoD agency counterparts for the exchange of information on OPSEC program matters. AFIWC will develop and maintain:

- The capability to accomplish multi-disciplined OPSEC surveys.
- OPSEC training aids and materials to support an active marketing and training program to be presented by OPSEC PMs in the field.
- A training course for OPSEC program managers and other personnel who perform OPSEC surveys.

A2.4.1. AFIWC will also make available to all Air Force units and supporting organizations current mission specific, foreign intelligence threat information. Threat information will identify current and potential adversaries and include foreign intelligence capabilities, intentions, resources, doctrine and state-of-the-art intelligence collection methods.

A2.5. Air Force Office of Special Investigations (AFOSI). AFOSI is the sole agency within the U.S. Air Force chartered to perform the counterintelligence mission. AFOSI will support OPSEC PMs and commanders with OPSEC survey support, Multi Disciplinary Counterintelligence (MDCI) Threat Assessments, planning and training assistance, and a complete range of studies, reports, and analytical products. AFOSI detachment commanders will assist their local commanders with access, as necessary, to threat information from sources outside the Air Force.

A2.6. Air Education and Training Command (AETC) Responsibilities Air Education and Training Command (AETC) will provide for a basic, but thorough, introduction of OPSEC to all new (military) Air Force members. The block of training must include:

- The purpose and value of the OPSEC concept.
- An overview of the process.
- An introduction to the application of OPSEC measures.

A2.6.1. OPSEC will be presented as “this is the way we do our day-to-day business in the United States Air Force.” AETC will also provide general OPSEC education, as appropriate, in all professional level courses. Professional level materials should include the purpose and use of the OPSEC concept, the process, complementing and conflicting concepts, OPSEC planning, and command responsibilities.

SOURCES OF OPSEC INDICATORS

NOTE: This list is NOT all inclusive. It is provided as a stimulus only. The only limit here is your own imagination!

A3.1. Operations Indicators:

- Stereotyped activities such as schedules, test preparations, range closures
- Visits of VIPs associated with a particular activity or technology
- Abrupt changes or cancellations of schedules
- Specialized equipment
- Specialized training
- Increased telephone calls, conferences, and longer working hours (including weekends)
- Rehearsals of operations
- Unusual or increased trips and conferences by senior officials

A3.2. Communications Indicators:

- Specialized and unique communications equipment
- Power sources
- Increases and decreases in communications traffic
- Call signs
- Transmitter locations

A3.3. Administrative Indicators:

- Military orders
- Distinctive emblems, logos, and other markings on personnel, equipment, and supplies
- Transportation arrangements
- Schedules, orders, flight plans, and duty rosters
- Leave cancellations

A3.4. Logistics and Maintenance Support Indicators:

- Unique sized and shaped boxes, tanks, and other containers
- Pre-positioned equipment
- Technical representatives
- Maintenance activity
- Unique or special commercial services
- Deviations of normal procedures
- Physical security arrangements

PROGRAM MANAGER (PM) DUTIES

A4.1. OPSEC Pms.

- Facilitating the implementation of OPSEC throughout their organization
- Integrating OPSEC into organizational plans and activities
- Advising commanders and other decision makers on OPSEC matters
- Coordinating on (and facilitating the development of) OPSEC plans and measures for operations, activities, and exercises
- Integrating OPSEC requirements into C2W and information warfare strategies
- Developing and maintaining the organization’s OPSEC program
- Ensuring all personnel receive appropriate OPSEC training
- Conducting annual OPSEC self-inspections and OPSEC appraisals (as directed)
- Providing OPSEC program requirements for intelligence and counterintelligence support
- Coordinating OPSEC requirements with public affairs officers
- Coordinating with activities which complement OPSEC
- Ensuring mission critical information is identified and controlled
- Assisting in determining operational requirements for security and guidelines for the release of information
- Determining guidelines for controlling mission critical information and sensitive activities
- Coordinating and facilitating OPSEC surveys
- Maintaining an effective rapport with foreign intelligence and counterintelligence agencies
- Forwarding recommendations for change or program modification to HQ USAF/XOOP through appropriate channels.

EXAMPLE OPSEC SELF-INSPECTION CHECKLIST

1. Has a unit or staff agency OPSEC officer or noncommissioned officer (NCO) been appointed in writing?

a. Is the appointee from the unit Plans or Operations element?

b. Has the identity of the OPSEC officer/NCO been forwarded to higher headquarters OPSEC offices of primary responsibility (OPR)?

c. Are visual aids identifying the OPSEC officer and NCO prominently displayed throughout the unit or staff agency?

d. Are the unit or staff agency OPSEC officer and NCO aware of their responsibilities?

e. Does the OPSEC officer/NCO attend and address OPSEC matters at unit security awareness and education meetings?

f. Has the unit OPSEC officer/NCO attended or requested to attend the USAF OPSEC Program Managers' Course through their MAJCOM, FOA or DRU OPSEC OPR?

2. Has the OPSEC officer/NCO established a continuity folder?

a. Are current editions of all instructions, pamphlets, and directives (JCS Pub 3-54, AFPD 10-11, AFI 10-1101, MAJCOM Sups) being maintained in support of the OPSEC program?

b. Does the unit have local directives which define unit OPSEC program requirements, responsibilities, and procedures?

3. Does the commander actively advocate, support, and implement OPSEC options in support of the operational mission and exercises?

a. Has the commander signed an OPSEC policy letter supporting the program?

b. Is the unit Critical Information (CI) reviewed and approved by the Commander?

c. Is OPSEC addressed at Commander's Call?

4. Does the unit OPSEC program promote active participation and involvement of all personnel?

a. Are OPSEC posters prominently displayed throughout the unit?

b. Are OPSEC education materials reaching all unit members?

c. Is the unit CI list tailored to each functional activity?

(1) Is the CI list specific, realistic, and current?

(2) Are unit or functional area CI lists easily accessible to unit members?

(3) Are unit members familiar with unit or functional area CI?

(4) Is the CI list unclassified to allow for maximum dissemination?

5. Does the unit OPSEC program include provisions for reviewing plans, operations orders (OPORD), and exercise scenarios?

a. Is current potential adversary threat data maintained and considered in plans and exercises?

b. Do unit plans or OPORDS, contain, as a minimum, the purpose and current definition of OPSEC, OPSEC Threat, and CI?

6. Are the interrelationships of OPSEC, communications security (COMSEC), computer security (COMPUSEC), physical security, and information security programs clearly understood by the OPSEC officer/NCO?

7. Has the unit OPSEC officer/NCO coordinated with other unit security managers (e.g., COMSEC, Information Security, COMPUSEC), to incorporate OPSEC concepts and lessons learned into security training sessions?

8. Has the unit OPSEC officer/NCO established and maintained liaison with the base or higher headquarters OPSEC Program Manager?

9. Is OPSEC training related to the unit mission, tailored to individual duties and responsibilities, and presented to newly assigned personnel within 90 days after arrival for duty?

10. Does unit OPSEC training contain the following:

a. The OPSEC methodology?

b. Duty related mission critical information and OPSEC indicators?

c. Foreign intelligence threat to the unit mission?

d. Individual responsibilities?

e. OPSEC and its relationship to IW/C2W?

11. Has the OPSEC officer/NCO submitted an annual OPSEC Status Report, if required by their respective MAJCOM or FOA?

12. Has an OPSEC survey or appraisal been conducted?

a. If yes:

(1) Are the results easily accessible?

(2) Have results been addressed through unit awareness programs?

(3) Has unit mission or CI changed significantly to warrant a new survey?

b. If no, has one been scheduled or requested?

13. Have actions been taken to act on recommendations or to correct weaknesses and deficiencies noted in the OPSEC survey?

14. Are all OPSEC recurring publications (e.g., the OPSEC update, COMSEC quarterly analyses, etc.) reviewed for OPSEC lessons learned?

15. Do official and unofficial feedback publications such as unit newsletters contain sensitive or classified information? If so, are they protected?

16. Do indexes for directives and operating instructions reveal sensitive operations or functions?

17. Do unclassified computer products disclose sensitive mission activity?

18. Are ADP products protected and destroyed as classified waste?

19. Are the OPSEC officer/NCO on distribution for telecommunications monitoring or AFOSI HUMINT Vulnerability Assessment reports involving their unit?

20. Are Quality Air Force (QAF) measures in place to determine program success and improvement?